UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/539,566	06/07/2005	Francois Bangui	0521-1027	5911

466 7590 09/16/2008

YOUNG & THOMPSON
209 Madison Street
Suite 500
ALEXANDRIA, VA 22314

EXAMINER	
SQUIRES, BRETT S	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
09/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/539,566	BANGUI, FRANCOIS	
	Examiner	Art Unit	
	BRETT SQUIRES	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *22-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *22-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 June 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *06/17/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Specification

1. The disclosure is objected to because of the following informalities: the various sections of the specification are not labeled with the appropriate section heading. Please see MPEP 608.01(a). Appropriate correction is required.

35 USC § 112, sixth paragraph

2. Claims 34-36, 39, 41-42, and 44 satisfy the three-pronged analysis necessary to invoke 35 U.S.C. § 112, sixth paragraph and accordingly these claims are interpreted as means-plus-function claims. The three-pronged analysis necessary to invoke 35 U.S.C. § 112, sixth paragraph is recited below:

A claim limitation will be presumed to invoke 35 U.S.C. 112, sixth paragraph, if it meets the following 3-prong analysis:

(A)the claim limitations must use the phrase "means for" or "step for;"

(B)the "means for" or "step for" must be modified by functional language; and

(C)the phrase "means for" or "step for" must not be modified by sufficient structure, material, or acts for achieving the specified function.

Claim Objections

3. Claims 22-24 and 26-44 are objected to because the claims are written as European style two-part claims including a "characterizing" clause. Please MPEP 2111.03, for the appropriate transitional phrases that define the scope of a claim with

respect to what unrecited additional components or steps, if any, are excluded from the scope of the claim. Appropriate correction is required.

Claims 31 and 41-42 are objected to for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 31 and 41-42 recite "and/or," this claim language causes ambiguity in determining what elements are required by the claims. The examiner respectfully points out that for examination purposes "and/or" is construed to mean or. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 30, 34-42 and 44 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 30 recites the limitation "its memory context card" in page 5 line 13 of the preliminary amendment submitted on June 17, 2005. There is insufficient antecedent basis for this limitation in the claim. Appropriate correction is required.

Claim 34 recites the means-plus-function claim elements: "means for moving said executable certificate to the host terminal," "comparison means for comparing the result obtained through the execution of the control instruction with the result expected from an authentic application," and "means which are capable, in the event of a positive

comparison, of continuing with the execution of the software application to be verified." The specification fails to disclose adequate corresponding structure for the above claim elements, thereby rendering claims 34-42 and 44 indefinite. Appropriate correction is required.

The specification does not recite any corresponding structure for the claimed "means for moving said executable certificate to the host terminal," and "means which are capable, in the event of a positive comparison, of continuing with the execution of the software application to be verified." The specification recites "comparison means for comparing the result of the execution of the executable certificate on the behaviour of the software application to be verified with the result expected from the behaviour of an authentic application," on page 6 lines 12-15, this recitation does not provide adequate corresponding structure for the claimed "comparison means for comparing the result obtained through the execution of the control instruction with the result expected from an authentic application."

35 U.S.C. 112, sixth paragraph states that a claim limitation expressed in means-plus-function language "shall be construed to cover the corresponding structure...described in the specification and equivalents thereof." "If one employs means plus function language in a claim, one must set forth in the specification an adequate disclosure showing what is meant by that language. If an applicant fails to set forth an adequate disclosure, the applicant has in effect failed to particularly point out and distinctly claim the invention as required by the second paragraph of section 112." *In re Donaldson Co.*, 16 F.3d 1189, 1195, 29 USPQ2d 1845, 1850 (Fed. Cir. 1994) (in banc).

Claim 35 recites the means-plus-function claim element "a means for communication with the secure circuit." The specification does not recite any corresponding structure for the above means-plus-function claim element, and thereby renders the claim element indefinite. Appropriate correction is required.

Claim 36 recites the means-plus-function claim element "means which is capable of validating or invalidating the authenticity of the software application." The specification does not recite any corresponding structure for the above means-plus-function claim element, and thereby renders the claim element indefinite. Appropriate correction is required.

Claim 36 recites the limitation "the signature produced by the series of control instruction" in page 7 lines 6-7 of the preliminary amendment submitted on June 17, 2005. There is insufficient antecedent basis for this limitation in the claim. Appropriate correction is required.

Claim 40 recites the improper Markush Group of "the host terminal belongs to the group formed by data processing apparatuses, digital television decoders, equipment for visualizing multimedia contents, micro-computers, smart cards, personal organizers, game consoles, mobile telephones or the like." The use of "or the like" when claiming a Markush Group is improper because "or the like" allows for inclusion of additional unrecited elements, and therefore renders the Markush Group indefinite. Appropriate correction is required.

Claim 44 recites the means-plus-function claim element "means which are capable of inserting the executable certificate into a first stream of data." The

specification does not recite any corresponding structure for the above means-plus-function claim element, and thereby renders the claim element indefinite. Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 22-23 and 25-44 are rejected under 35 U.S.C. 102(e) as being anticipated by McCarroll (US 2003/0196102).

Regarding Claim 22:

McCarroll discloses a method of verifying the integrity of a software application ("Software code for a game" See paragraph 26) which is executable in a host terminal ("Computer system" See fig. 1 ref. no. 100 and paragraph 20) that determines at least one series of control instructions forming an executable certificate ("A digitally signed portion of software code for a game" See paragraph 26) for the software application, which can be executed by the host terminal during the execution of the software application to be verified ("The digitally signed portion of software code can be the table of contents, the application itself, executable files, boot bios, and any other sensitive

data." See paragraph 26), on the host terminal executing the software application to be verified ("The processing circuitry reads a portion of software code." See paragraph 28), receiving the executable certificate ("The portion of software code being read is one of the portions of code that has been digitally signed." See paragraph 28), executing the series of control instruction for the executable certificate in the memory context of the host terminal ("The signature file corresponding to the digitally signed portion of software code is decrypted and the digitally signed portion of software code is hashed in to first message digest." See paragraphs 28-30), comparing the result thus obtained through the execution of the control instructions with the result expected from an authentic software application ("The first message hash is compared to a second message digest from the decrypted signature file." See paragraph 30), and in the event of a positive comparison continuing with the execution of the software application ("The software code for game will continuing executing if the software is determined to be valid." See paragraph 30)

Regarding Claim 23:

McCarroll discloses the host terminal has a processor ("CPU" See fig. 1 ref. no. 110) and the series of control instructions forming the certificate is coded in a language which can be interpreted by the processor of the host terminal (The processing circuitry reads the digitally signed portion of software code." See paragraph 28).

Regarding Claim 25:

McCarroll discloses the executable certificate includes a portion of the processing necessary for the satisfactory operation of the authentic program ("The

digitally signed portion of software code can be the table of contents, the application itself, executable files, boot bios, and any other sensitive data." See paragraph 26).

Regarding Claim 26:

McCarroll discloses a card with the memory context of the authentic software application during the course of execution ("Small card-like media using Sony MagicGate or Sony Memory Stick technology." See fig. 1 ref. no. 108 and paragraph 21), and to determine from the values of this memory card the series of control instructions intended to form the executable certificate ("A digitally signed executable file is loaded from the small card-like media by the processing circuitry and the cryptography unit determines if the file is valid." See paragraph 32)

Regarding Claim 27:

McCarroll discloses the executable certificate for the host terminal emanates from an electronic processing circuit ("Remote server" See fig. 3 ref. no. 134) which is physically separated from the host terminal ("The computer system downloads one or more portions of software code that have been digitally signed from the remote server." See paragraph 35).

Regarding Claim 28:

McCarroll discloses the recovery of the execution values of the memory context is effected by reading the values at the addresses of the various portions of the memory of the host terminal, these portions containing the executable instructions and the data intrinsic to the application to be verified ("The processing circuitry reads a portion of software code from the storage device, the software that is read is can be a portion of

software code that has been digitally signed or a portion of software code that has not been digitally signed." See paragraphs 26-28).

Regarding Claim 29:

McCarroll discloses the result obtained by the execution of the series of control instructions produces a signature for the application to be verified ("A first message digest" See paragraph 30), this signature being calculated by the series of control instructions uses the vales of the memory context of the software application to be verified during the course of execution of the application ("The cryptography unit hashes a portion of software code, such as the table of contents, the applications itself, the executable files, the boot bios, or any other sensitive data, into a first message digest." See paragraph 30)

Regarding Claim 30:

McCarroll discloses the software application has instruction which permit the series of control instruction to be loaded and executed in a memory context card ("PC card or PCMCIA card" See fig. 5a ref. no. 120) by substituting at least one address for executing an instruction of the software application by at least one instruction address of the series of instructions which form the certificate ("The PC card includes a cryptography unit for ensuring the integrity of the copy protection and the integrity of the machine code of system software." See fig. 5a ref. no. 122 and paragraphs 24 and 45).

Regarding Claim 31:

McCarroll discloses the series of control instructions is selected in such a manner that the state of the memory context of one software application after the execution of

the series of control instruction is identical or without any modification to the state of the memory context of the software application prior to the execution of the series of control instructions ("The creation of message digests using; the table of contents, the applications itself, the executable files, the boot bios, or any other sensitive data of software code for a game does not alter the software code for a game." See paragraphs 30-32).

Regarding Claim 32:

McCarroll discloses the series of instructions forming the certificate is transported into a stream of data necessary for the execution of the software application to be verified ("One or more portions of software code that have been digitally signed can be downloaded by the computer system." See paragraph 35).

Regarding Claim 33:

McCarroll discloses the software application to be verified is wholly or partially encoded ("The contents of the computer readable medium could also be encrypted." See fig. 1 ref. no. 108 and paragraph 27), the correct deciphering software application being achieved in the event of integrity of the software application to be verified ("The encrypted contents of the computer readable medium are digitally signed and when the encrypted contents are determined to be valid the encrypted content are decrypted, however when the encrypted contents are determined to be invalid the operation of the system is prevented and thus the contents are not decrypted." See fig. 2a-2b and paragraphs 26-30)

Regarding Claims 34 and 40:

McCarroll discloses a system (See fig. 1 ref. no. 100) having a processing means ("Processing Circuit" See fig. 1 ref. no. 104) capable of determining at least one series of control instruction for the software application which can be executed by the system during the execution of the software applications, the series of control instructions forms an executable certificate ("A digitally signed portion of software code for a game" See paragraph 26) of the software application, means for moving the executable certificate to the system ("Storage Device having removable computer readable media" and "Modem" See fig. 1 ref. nos. 102, 132 and paragraph 21) and executing means ("Cryptography Unit" See fig. 1 ref. no. 122 and paragraphs 29-30) for executing the series of instructions forming the certificate on the system during the execution of the software application, comparison means ("The cryptography unit compares the first message digest with the second message digest." See paragraphs 29-30) for comparing the result obtained through the execution of the control instruction with the result expected from an authentic application, and means which are capable, in the event of a positive comparison of continuing with the execution of the software application to be verified ("The cryptography unit indicated whether or not a portion of code is valid." See paragraph 30).

Regarding Claim 35:

McCarroll discloses a smart card ("PC card or PCMCIA card" See fig. 5a ref. no. 120) that is capable of containing the series of control instruction forming the certificate, the system is provided with a reader ("Slot interface" See fig. 5a ref. no. 160) for reading the smart card, and means for executing the software application ("Cryptography Unit"

See fig. 1 ref. no. 122 and paragraphs 29-30) are provided in the smart card the series of instruction forming the certificate during the execution of the software application to be verified ("The digitally signed portion of software code can be the table of contents, the application itself, executable files, boot bios, and any other sensitive data." See paragraph 26).

Regarding Claim 36:

McCarroll discloses the system is capable of returning to the smart card a signature ("A second message digest is contained in the signature filed with digitally signed portion of software code and the second message digest is sent from the system to the PC card." See paragraphs 28-30) produced by the series of control instructions and the smart card has a software verifying means ("The cryptography unit indicated whether or not a portion of code is valid." See paragraph 30) which is capable of validating or invalidating the authenticity of the software application to be verified in dependence on the result of the comparison between the signature produced by the series of control instruction and a value for the signature which is known and previously stored in the smart card ("The cryptography unit compares the first message digest with the second message digest." See paragraphs 29-30).

Regarding Claims 37 and 39:

McCarroll discloses the smart card is capable of preventing the operation of the software application of the system ("The cryptography unit compares the created message digest with the decrypted digest and if the digests do not match the operation of the system is prevented" See paragraph 32).

Regarding Claim 38:

McCarroll discloses in the event of a non-transmission of the signature in conformity with predetermined conditions ("Swap trick type of copy protection defeat," See paragraph 32), the smart card is capable of modifying the operation of the software application to be verified ("The cryptography unit compares the created message digest with the decrypted digest and if the digests do not match the operation of the system is prevented" See paragraph 32).

Regarding Claims 41 and 42:

McCarroll discloses the processing means are capable of determining a plurality of executable certificates which differ from one another according to a selected rate or condition ("The processing circuit reads digitally signed portion of software code such as the table of contents, the application itself, executable files, boot bios, and any other sensitive data." See paragraph 26).

Regarding Claim 43:

McCarroll discloses inserting the executable certificate into a first steam of data ("Table of Contents for software code" See paragraphs 28-29) and of processing through encoding a second stream of data ("Encrypted signature file for the table of contents" See paragraph 29) necessary for satisfactory operation of the software application to be verified prior to the second stream not being obtained for processing through the software application to be verified ("Prior to the computer readable media being inserted into the system at least a portion of the software code for the game is digitally signed with a key." See paragraph 26).

Regarding Claim 44:

McCarroll discloses means which are capable of inserting the executable certificate ("Manufacture's equipment for mastering DVDs" See paragraph 26) into a first stream of data ("Table of Contents for software code" See paragraphs 28-29) and means for processing through encoding ("Manufacture's equipment for mastering DVDs" See paragraph 26) a second stream of the data ("Encrypted signature file for the table of contents" See paragraph 29) necessary for the satisfactory operation of the software application to be verified prior to the second stream not being obtained for processing through the software application to be verified.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claim 24 is rejected under 35 U.S.C. 103(a) as being obvious over McCarroll (US 2003/0196102) in view of Yach et al. (US 2004/0025022).

McCarroll discloses the above stated method of verifying the integrity of a software application ("Software code for a game" See paragraph 26) which is executable in a host terminal ("Computer system" See fig. 1 ref. no. 100 and paragraph 20).

McCarroll does not disclose the host terminal is provided with a virtual machine which capable of emulating a processor and that the series of control instruction forming the certificate is coded in a language which can be interpreted by the virtual machine.

Yach discloses a method for code signing that has a virtual machine for verifying the authenticity of the digital signature of a software application (See paragraphs 8-9).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of verifying the integrity of a software application disclosed by McCarroll to include a virtual machine for verifying the authenticity of the digital signature of a software application in order to protect the user from unreliability of software downloaded from the internet (See Yach paragraph 5).

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRETT SQUIRES whose telephone number is (571) 272-8021. The examiner can normally be reached on 9:00am - 5:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BS/

/Christopher A. Revak/
Primary Examiner, Art Unit 2131